Using Malware Analysis to Evaluate Botnet Resilience

Rossow, C.

2013

document version
Publisher's PDF, also known as Version of record

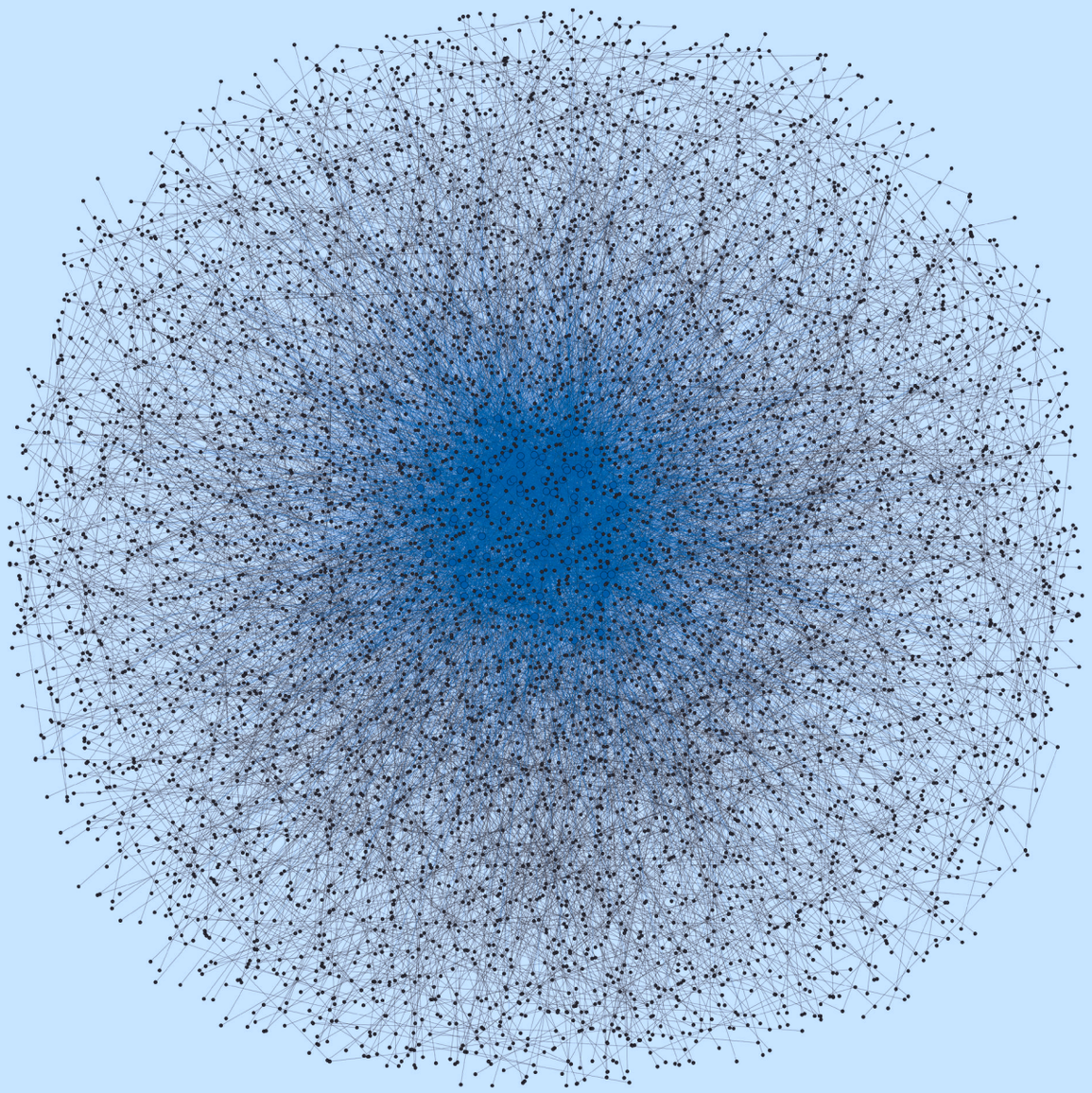
Botnets, networks of malware-infected PC systems, impose a threat to millions of users. In this PhD thesis, Christian Rossow analyzes the resilience of these malicious networks. By the help of the dynamic malware analysis system SANDNET, he explores the infrastructures which keep botnets operable over many years. The thesis covers two aspects of botnet resilience. First, the infrastructures that are being used for malware installations are analyzed. Second, this thesis shows how botmasters use overly resilient infrastructures in cutting-edge botnets, such as bots organized in peer-to-peer topologies. The results lead to the conclusion that botnet mitigation – unless addressed properly – will become overly complex, if not even infeasible, in the near future.

VU UNIVERSITY AMSTERDAM

C. Rossow

Using Malware Analysis to Evaluate Botnet Resilience

Using Malware Analysis to Evaluate Botnet Resilience



Christian Rossow